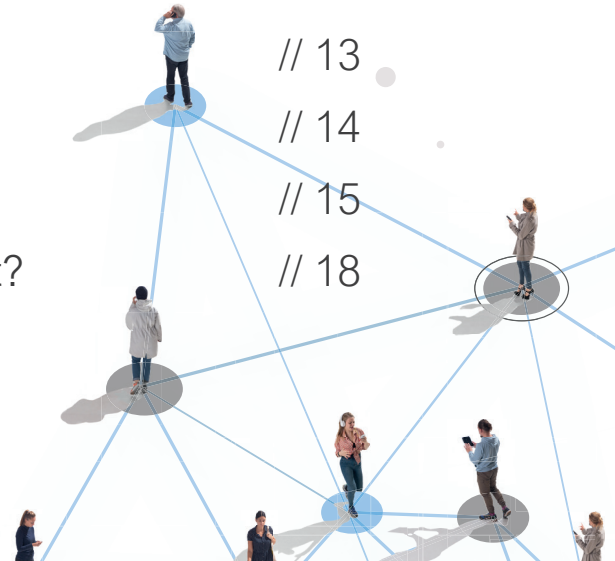
how to

MOBILE DEVICE MANAGEMENT VS. MOBILE APPLICATION MANAGEMENT
EINSTIEG IN DIE MOBILE GERÄTEVERWALTUNG

INHALT



BYOD & COPE

Mobile Geräte zentral verwalten

Die Nutzung mobiler Endgeräte ist im Arbeitsalltag zum Standard geworden. Bring your own device (BYOD) oder Corporate owned private enabled (COPE) zählen dabei zu den beliebtesten Modellen für die Bereitstellung von Smartphones und Tablets. So greifen immer mehr Mitarbeitende sowohl mit firmeneigenen als auch mit privaten Tablets oder Smartphones auf das Unternehmensnetzwerk zu.

Die Konsequenz: Auch die Unternehmenssoftware wird zunehmend als mobile Anwendung und nicht mehr als natives Web-Frontend oder Client-/Serveranwendung bereitgestellt. Die Nutzung von Apps birgt jedoch auch ein erhebliches Sicherheitsrisiko.

Die IT-Abteilung steht also vor großen Herausforderungen: Wie kann die Vielfalt mobiler Geräte und Anwendungen kontrolliert werden? Und wie verhält es sich um Datenschutz, Informationssicherheit und Security?

MOBILE DEVICE MANAGEMENT

MOBILE DEVICE MANAGEMENT

Zentrale Verwaltung und sicherer Einsatz mobiler Endgeräte

Mobile Device Management (MDM) ist der Oberbegriff für softwarebasierte Lösungen zur zentralen Verwaltung und dem sicheren Einsatz mobiler Endgeräte. Die einfache Registrierung und Konfiguration der Geräte reduziert die Arbeitsbelastung der IT erheblich. MDM-Systeme kümmern sich um die Ersteinrichtung und die Verwaltung und ersparen dem Administrator, alle Einstellungen für jedes einzelne Gerät manuell zu konfigurieren und die Geschäftsanwendungen einzeln zu installieren. Darüber hinaus ermöglichen MDM-Lösungen die Daten auf den Endgeräten zu kontrollieren und Probleme aus der Ferne zu beheben. Dies ist ideal für die Geräteverwaltung von Unternehmen, deren Mitarbeitende auch remote arbeiten.

FÜR WELCHE UNTERNEHMEN KOMMT EIN MDM IN FRAGE?

Die Implementierung von MDM-Systemen ist mittlerweile Standard für alle Unternehmen, die einen angemessenen Datenschutz und eine sichere Integration mobiler Geräte in ihre IT-Architektur gewährleisten wollen. Für Unternehmen, die Smartphones und Tablets einsetzen lohnt sich ein MDM selbst dann, wenn die Mitarbeitenden nur einfache Funktionen wie geschäftliche E-Mails lesen nutzen.

ALLE FUNKTIONEN IM ÜBERBLICK

Mobiles Management: MDM-Lösungen erleichtern die Verwaltung und den Support mobiler Geräte. Sie ermöglichen die Kontrolle der Geräte und prüfen, ob diese über das erforderliche Betriebssystem und die benötigten Anwendungen verfügen.

Identity und Access Management: Damit Mobilgeräte sicher verwaltet werden können, ist ein effektives Identitäts- und Zugriffsmanagement (IAM) erforderlich. Ein IAM dient dazu, die Benutzeridentitäten eines Geräts zu verwalten. So kann innerhalb eines Unternehmens der Zugang eines jeden Benutzers vollständig über Funktionen wie Single-Sign-On (SSO), Mehrfaktorauthentifizierung und rollenbasierten Zugriff reguliert werden.

Policy Management: Die Durchsetzung von Richtlinien gemäß den Unternehmensanforderungen ermöglicht den effektiven Schutz von Daten und Geräten. Es wird festgelegt, mit welchen Konfigurationen und Restriktionen Apps auf mobilen Endgeräten installiert werden dürfen.

Daten- und Gerätesicherheit: Mit MDM-Systemen können Sicherheitsmaßnahmen zum Schutz der Geräte und der darauf gespeicherten Daten erzwungen werden. Hierzu zählen beispielsweise eine Verschlüsselung der Daten und sichere Passwörter. Falls ein Gerät verloren geht oder gestohlen wird, kann es aus der Ferne gesperrt und die darauf enthaltenen Unternehmensdaten gelöscht werden.

Automatisierung: Unternehmen, die eine Vielzahl an Geräten verwalten, profitieren von der automatisierten Konfiguration dank Apple Business Manager, Android Zero-Touch-Enrollment oder Samsung Knox Mobile Enrollment. Mithilfe dieser Programme können alle erforderlichen Einstellungen und Apps automatisch auf den Geräten der Mitarbeitenden ausgerollt werden.

Remote-Wartung: MDM-Lösungen ermöglichen der IT-Abteilung Geräte aus der Ferne zu warten, ohne dass der Mitarbeitende extra ins Büro fahren muss. Software-Updates, Konfigurationen, Gerätediagnosen und Troubleshooting können remote durchgeführt werden. Dadurch wird Zeit gespart und Aufwände werden reduziert.

VORTEILE VON MDM-SYSTEMEN

Zentrale Verwaltung & Kontrolle: Mit einem MDM-System behalten IT-Administratoren den Überblick über alle sich im Einsatz befindenden Endgeräte und deren Lebenszyklus. Neue Geräte können schnell und effizient zum Unternehmensnetzwerk hinzugefügt werden. Darüber hinaus weiß die IT stets, wie hoch die Sicherheitsstufe des jeweiligen Endgeräts ist und kann alle Unternehmensdaten löschen, wenn ein Mitarbeitender aus dem Unternehmen ausscheidet.

Erhöhte Produktivität & niedrige Kosten: Durch die Automatisierung von Geräteregistrierungen und -konfigurationen werden Zeit und Kosten gespart. Auch die Fehler, die bei einem manuellen Deployment auftreten können, werden dabei verhindert. Die Mitarbeitenden müssen keine Zeit für die Einrichtung ihrer Geräte aufwenden und nicht extra die interne IT-Abteilung aufsuchen. Mit einem MDM haben sie von Beginn an vorkonfigurierte Geräte mit Zugriff auf alle für ihre Arbeit erforderlichen Daten und Anwendungen.

Datenschutz & Compliance: Seit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) müssen Unternehmen für die Verarbeitung personenbezogener Daten entsprechende technische und organisatorische Maßnahmen ergreifen. MDM-Lösungen helfen Unternehmen dabei, die Richtlinien zu erfüllen. Mit ihnen können mobile Endgeräte sicher genutzt und Unternehmensdaten geschützt werden. Über die MDM-Konsole werden Sicherheitsmaßnahmen einheitlich durchgesetzt und überwacht. Darüber hinaus ermöglicht ein MDM die sofortige Ergreifung von Notfallmaßnahmen z.B. indem ein verlorenes Gerät per Standortverfolgung lokalisiert und Unternehmensdaten aus der Ferne gelöscht werden (Remote Wipe).

VERWALTUNG VERSCHIEDENER ENDGERÄTE

MDM-Systeme dienen vorrangig der Verwaltung von Smartphones und Tablets. Es gibt jedoch auch Lösungen, die die Verwaltung von Laptops, Desktops und anderen Geräten ermöglichen. Welches Betriebssystem unterstützt wird, variiert von Anbieter zu Anbieter. Während einige Anbieter auf Apple- oder Android-Geräte spezialisiert sind, unterstützen andere eine größere Bandbreite von Betriebssystemen, wie zum Beispiel Windows, Chromebook oder Linux.

Verwaltungslösungen mit einem plattformübergreifenden Support, werden als Enterprise Mobility Management (EMM) oder Unified Endpoint Management (UEM) bezeichnet.

MOBILE APPLICATION MANAGEMENT

MOBILE APPLICATION MANAGEMENT

Kontrolle der Apps auf mobilen Endgeräten

Da immer mehr Mitarbeitende mobile Endgeräte sowohl privat als auch geschäftlich nutzen, ist ein Mobile Application Management (MAM) unerlässlich, um neben der ordnungsgemäßen Verwaltung der Geräte, auch die Sicherheit der Anwendungen zu gewährleisten.

Ein MAM ermöglicht die Kontrolle der Apps auf allen mobilen Geräten, die in einem Unternehmen eingesetzt werden. Es handelt sich dabei um eine Software, mit der die IT die Anwendungen auf den betreffenden mobilen Geräten aus der Ferne überwachen und steuern kann.

Mit einem MAM können außerdem Richtlinien für das Anwendungsmanagement umgesetzt werden. Diese verhindern die Installation und Nutzung nicht autorisierter Apps, legen den eingeschränkten Benutzerzugriff auf bestimmte Vorgänge und Daten für bestimmte Nutzergruppen fest und ermöglichen die Entwicklung eines zentralisierten internen App-Stores.

VORTEILE VON MAM

Enterprise App Store: MAM-Lösungen ermöglichen Unternehmen App-Kataloge zu erstellen, die auf ihre Anforderungen zugeschnitten sind. So können IT-Administratoren nahtlos verschiedene öffentliche und unternehmenseigene Anwendungen für ihre Mitarbeitenden bereitstellen.

Abteilungsspezifische Bereitstellung: Unternehmen arbeiten mit einer Vielzahl von Teams mit unterschiedlichen Anwendungsanforderungen. Oftmals ist es nicht zwingend erforderlich, dass alle Teams in einem Unternehmen sämtliche verfügbare Anwendungen nutzen. Mit MAM können Admins Anwendungen individuell für verschiedene Benutzergruppen bereitstellen.

Automatisierte Installation: Anwendungen, die für das Unternehmen bzw. die jeweilige Abteilung obligatorisch sind, können automatisch auf den Geräten der Mitarbeitenden installiert werden. Da dieser Prozess vorkonfiguriert werden kann, wird die IT-Abteilung entlastet und die Mitarbeitenden müssen sich nicht mit komplexen Installationsverfahren befassen.

Zentrale Konfiguration: MAM-Lösungen ermöglichen Anwendungen entsprechend der Geschäftsanforderungen zu konfigurieren. Die Konfigurationen können auf die gesamte Geräteflotte des Unternehmens übertragen werden.

Geplante Updates: Bei einem effizienten App-Management geht es nicht nur um die Bereitstellung und Installation von Apps. IT-Administratoren müssen sicherstellen, dass die installierten Apps auf den Geräten der Mitarbeitenden immer auf dem neuesten Stand sind,

um maximale Performance zu gewährleisten und Cyberrisiken zu minimieren. MAM-Lösungen helfen dabei, den Überblick zu behalten und Updates rechtzeitig zu planen.

Verbesserte Sicherheit: Unternehmens-Apps werden von persönlichen Apps getrennt und vor unerwünschten Zugriffen gesichert. Darüber hinaus werden die in den Anwendungen gespeicherten sensiblen Unternehmensdaten vor unrechtmäßiger Weitergabe und Missbrauch geschützt.

Erhöhte Effizienz: Admins haben die Möglichkeit Unternehmensanwendungen von einer einzigen Konsole aus zu verwalten, überwachen, sichern, verteilen und zu aktualisieren sowie verschiedene Routineaufgaben zu automatisieren. Außerdem wird die Effizienz der Mitarbeitenden durch die die Verfügbarkeit von Unternehmensanwendungen auf ihren Firmen- oder Privatgeräten, unabhängig von ihrem Standort, erhöht.

ALLE FUNKTIONEN IM ÜBERBLICK

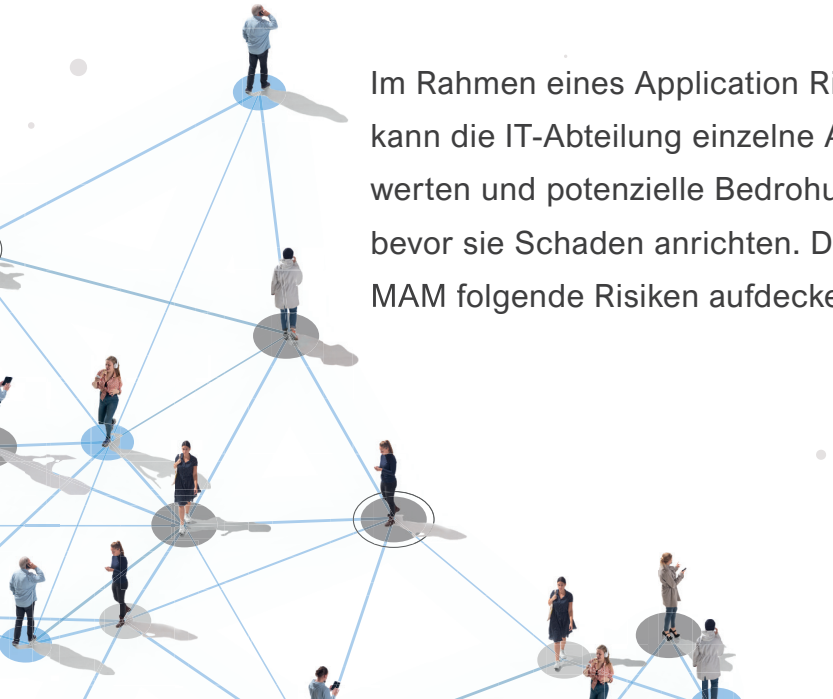
Je nach MAM-Lösung kann der Funktionsumfang unterschiedlich sein. Wichtige Funktionen des Mobile Application Managements sind:

FUNKTIONEN

- zentral gesteuerte Installation der Software und Anwendungen
- Konfiguration der Anwendungseinstellungen
- individuelles Branding der Anwendungen
- Authentifizierung der Anwender und Ressourcen
- sicherer Datenaustausch zwischen Unternehmensanwendungen
- Bereitstellung und Konfiguration sicherer VPN-Verbindungen
- Remote Datenverschlüsselung, Datenlöschung und Anwendungsdeaktivierung
- Lizenzierung und Inventarisierung von Software
- Application Lifecycle Management (ALM)
- Einspielen von Updates und Patches
- Logging der Anwenderaktivitäten
- Nutzungsanalysen

APP RISK MANAGEMENT

Mit der zunehmenden Nutzung mobiler Anwendungen nimmt auch das Risiko für Fehlfunktionen und Sicherheitsprobleme zu. Denn im App-Entwicklungsprozess können sich schnell codebasierte Fehler einschleichen, die für Unternehmen weitreichende Folgen haben. So können Daten abgegriffen werden, wenn die Datenübertragung in einer App nicht verschlüsselt ist oder es kommt zu einer Übertragung personenbezogener Daten an Staaten, die nicht DSGVO-gebunden sind, was zu erheblichen Datenschutzproblemen führt.



Im Rahmen eines Application Risk Management, kann die IT-Abteilung einzelne Anwendungen bewerten und potenzielle Bedrohungen evaluieren, bevor sie Schaden anrichten. Dabei kann das MAM folgende Risiken aufdecken:

- Verstöße gegen Datenschutzbestimmungen
- unkontrollierter Datenabfluss zu unternehmensfremden Servern
- Datenschutzverstöße durch Zugriff auf personenbezogene Daten
- Datensicherheitsverstöße durch unsichere Datenübertragung und unzulässige Serverstandorte
- unzulässige Verbindungen und Datenübertragungen an Dritte

Diese Informationen werden dem MDM zur Verfügung gestellt. Im Anschluss hat der Admin die Möglichkeit, die Anwendungen zu filtern sowie Positiv- und Negativlisten zu erstellen. Ergebnis ist ein App-Katalog, der den Anforderungen an Compliance und Datenschutz gerecht wird und die Gefahren für die IT-Security minimiert.

MDM VS. MAM

MDM VS. MAM

Unterschiede & Gemeinsamkeiten

Die Grenze zwischen MDM und MAM sind mittlerweile fließend. Während die beiden Lösungen ursprünglich als separate Produkte vermarktet wurden, sind sie heute in der Regel beide in Enterprise-Mobility-Management (EMM)- oder Unified-Endpoint-Management (UEM)-Produktsuiten enthalten.

Zu den zentralen Gemeinsamkeiten und Unterschieden zwischen MDM und MAM gehören:

ANWENDUNGSFALL

- Ein MDM ist sinnvoll, wenn die IT-Abteilung die vollständige Kontrolle über das Gerät haben soll. Bei BYOD-Geräten ist dies jedoch in der Regel nicht möglich.
- Ein MAM ist deshalb vor allem für BYOD-Geräte üblich, da hier nur bestimmte Anwendungen kontrolliert werden, wie z. B. Apps, die ausschließlich für geschäftliche Zwecke genutzt werden.

APP-VERWALTUNG

- MDM steuert Anwendungen durch Kontrolle des Geräts
- MAM steuert Apps mit bestimmten Funktionen

APP-WRAPPING UND CONTAINERISIERUNG

Sowohl MAM- als auch MDM-Lösungen bieten Funktionen für App-Wrapping und App-Containerisierung. Mithilfe dieser Technologien kann die IT-Abteilung Apps auf verwalteten Geräten kontrollieren, sichern und aktualisieren.

BENUTZER- UND GRUPPEN-AUTHENTIFIZIERUNG UND -AUTORISIERUNG:

Die Zugriffsverwaltung ist sowohl in MDM- als auch in MAM-Lösungen enthalten.

FAZIT

Welche Lösung ist für mein Unternehmen am besten geeignet?

MDM ist eine Methode zum Schutz und zur Kontrolle mobiler Geräte wie Smartphones und Tablets. Die Software ist oft für mehrere Betriebssysteme, wie iOS und Android, ausgelegt und eignet sich vor allem für COPE-Modelle. Für jedes registrierte Gerät wird ein Profil erstellt, mit dem Unternehmen die Geräte aus der Ferne verfolgen, sperren, sichern, verschlüsseln und bei Bedarf löschen können.

Im Gegensatz dazu schützt MAM die Anwendungen auf diesen Geräten, die für den Zugriff auf Unternehmensdaten, wie Outlook, SharePoint und OneDrive, verwendet werden. Diese Methode ist ideal für BYOD-Szenarien, denn MAM-Systeme ändern nichts an der Funktionsweise des Geräts, allerdings machen sie mobile Anwendungen sicherer und einfacher zu installieren. IT-Administratoren können mit MAM-Systemen Geschäftsanwendungen vorkonfigurieren, sie auf eine Flotte von Geräten übertragen sowie regelmäßige Wartung und Updates durchführen, Apps auf Geräten installieren oder entfernen und vieles mehr.

Sowohl MDM- als auch MAM-Lösungen sind also für die Verwaltung und den Schutz von geschäftlich genutzten Geräten wichtig.Auf dem Markt ist eine Vielzahl von MAM- und MAD-Lösungen erhältlich. Microsoft Intune beispielsweise ist ein cloudbasierter Dienst zur Verwaltung von Mobilgeräten und Apps, zum Schalten von Datenschutzrichtlinien, sowie zur Absicherung hinsichtlich Sicherheitsanforderungen.